

AN ALGORITHM FOR COMPUTING THE REDUCTION MOD p OF 2-DIMENSIONAL CRYSTALLINE REPRESENTATIONS

by

Laurent Berger

Abstract. — We give an algorithm for computing the reduction modulo p of 2-dimensional crystalline representations of $\text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. This algorithm relies on Fontaine's theory of (φ, Γ) -modules as well as the theory of Wach modules. It is rather explicit and can be implemented using standard mathematical software.

Contents

Introduction.....	1
1. (φ, Γ) -modules and Wach modules.....	4
2. Matrix lifting results.....	5
3. Proof of the main theorem.....	6
4. Identifying mod p representations.....	7
References.....	8

Introduction

Let p be a prime number $\neq 2$ and E a finite extension of \mathbf{Q}_p with ring of integers \mathcal{O}_E and maximal ideal \mathfrak{m}_E and uniformizer π_E and residue field k_E . If $k \geq 2$ and $a_p \in \mathfrak{m}_E$, let D_{k,a_p} be the filtered φ -module given by $D_{k,a_p} = Ee_1 \oplus Ee_2$ where :

$$\begin{cases} \varphi(e_1) = p^{k-1}e_2 \\ \varphi(e_2) = -e_1 + a_p e_2 \end{cases} \quad \text{and} \quad \text{Fil}^i D_{k,a_p} = \begin{cases} D_{k,a_p} & \text{if } i \leq 0, \\ Ee_1 & \text{if } 1 \leq i \leq k-1, \\ 0 & \text{if } i \geq k. \end{cases}$$

By the theorem of Colmez-Fontaine (théorème A of [CF00]), there exists a crystalline E -linear representation V_{k,a_p} of $\text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ such that $D_{\text{cris}}(V_{k,a_p}^*) = D_{k,a_p}$ where V_{k,a_p}^* is the dual of V_{k,a_p} . The representation V_{k,a_p} is crystalline, irreducible, and its Hodge-Tate weights are 0 and $k-1$. Let T denote a $\text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ -stable lattice of V_{k,a_p} and let \overline{V}_{k,a_p}

2000 Mathematics Subject Classification. — 11F, 11S, 11Y.

Key words and phrases. — Galois representations, (φ, Γ) -modules, Wach modules.

be the semisimplification of $T/\pi_E T$. It is well-known that \overline{V}_{k,a_p} depends only on V_{k,a_p} and not on the choice of T .

We should therefore be able to describe \overline{V}_{k,a_p} in terms of k and a_p but this seems to be a difficult problem. Note that it is easy to make a list of all semisimple 2-dimensional k_E -linear representations of $\text{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$: they are twists of $\text{ind}(\omega_2^r)$ (in the notation of [Bre03]) for some $r \in \mathbf{Z}$ or direct sums of two characters.

If $2 \leq k \leq p$, then the theory of Fontaine-Laffaille gives us $\overline{V}_{k,a_p} = \text{ind}(\omega_2^{k-1})$. If $k = p+1$ or $k \geq p+2$ and $v_p(a_p) > \lfloor (k-2)/(p-1) \rfloor$, then theorem 4.1.1, remark 4.1.2 and proposition 4.1.4 of [BLZ04] show that $\overline{V}_{k,a_p} = \text{ind}(\omega_2^{k-1})$. For other values of a_p we can get a few additional results by using the p -adic Langlands correspondence (see [BG09] or conjecture 1.5 of [Bre03], combined with [Ber05]) or by computing the reduction in specific cases using congruences of modular forms (Savitt-Stein and Buzzard, see for instance §6.2 of [Bre03]). However, no general formula is known or even conjectured. The purpose of this article is to give an algorithm which can be programmed and which, given the data of k and $a_p \bmod \pi_E^n$, will return \overline{V}_{k,a_p} if n is large enough.

This algorithm is based on Fontaine's theory of (φ, Γ) -modules (see A.3 of [Fon90]) and its refinement for crystalline representations, the theory of Wach modules (see [Ber04]). In order to give the statement of this article's main theorem, we give a few reminders about the theory of (φ, Γ) -modules for k_E -linear representations. Let Γ be a group isomorphic to \mathbf{Z}_p^\times via a map $\chi : \Gamma \rightarrow \mathbf{Z}_p^\times$. The field $k_E((X))$ is endowed with a k_E -linear frobenius φ given by $\varphi(f)(X) = f(X^p)$ and an action of Γ given by $\gamma(f)(X) = f((1+X)^{\chi(\gamma)} - 1)$. A (φ, Γ) -module (over k_E) is a finite dimensional $k_E((X))$ -vector space endowed with a semilinear frobenius whose matrix satisfies $\text{Mat}(\varphi) \in \text{GL}_d(k_E((X)))$ in some basis and a commuting semilinear continuous action of Γ . By a theorem of Fontaine (see A.3.4 of [Fon90]), the category of (φ, Γ) -modules over k_E is naturally isomorphic to the category of k_E -linear representations of $\text{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$. The group Γ is topologically cyclic (at least if $p \neq 2$) so that a (φ, Γ) -module is determined by two matrices P and G , the matrices of φ and of a topological generator γ of Γ in some basis. In the sequel, we denote by $\text{rep}(P, G)$ the k_E -linear representation associated to the (φ, Γ) -module determined by P and G .

If $f(X) \in \mathcal{O}_E[[X]]$, set $\varphi(f)(X) = f((1+X)^p - 1)$ so that in particular, $\varphi(X) = XQ$ where $Q = \Phi_p(1+X)$, and let Γ act on $\mathcal{O}_E[[X]]$ by $\eta(f)(X) = f((1+X)^{\chi(\eta)} - 1)$. Recall that γ is a fixed topological generator of Γ ; we write $\gamma_1 = \gamma^{p-1}$ so that $\chi(\gamma_1)$ is a topological generator of $1+p\mathbf{Z}_p$ and if G is the matrix of γ in some basis, then the matrix of γ_1 is $G_1 = G\gamma(G) \cdots \gamma^{p-2}(G)$.

Definition. — Let $W_{k,a_p}(n)$ be the set of pairs of matrices (P, G) with $P, G \in M_2(\mathcal{O}_E[[X]]/(\pi_E^n, \varphi(X)^k))$ satisfying the following conditions :

1. $P\varphi(G) = G\gamma(P)$;
2. $G = \text{Id} \bmod X$;
3. $\det(P) = Q^{k-1}$ and $\text{Tr}(P) = a_p \bmod X$;
4. if $\Pi(Y) = (Y - 1)(Y - \chi(\gamma_1)^{k-1})$, then $\Pi(G_1) = 0 \bmod Q$.

If $(P, G) \in W_{k,a_p}(n)$, then we denote by \overline{P} and \overline{G} two matrices in $M_2(k_E[[X]])$ which are equal modulo $\varphi(X)^k$ to the reductions modulo π_E of P and G (note that in $k_E[[X]]$, we have $\varphi(X) = X^p$). They then satisfy the relation $\overline{P}\varphi(\overline{G}) = \overline{G}\gamma(\overline{P}) \bmod \varphi(X)^k$ and in proposition 2.1 below, we prove that we can modify \overline{G} modulo X^k so that $\overline{P}\varphi(\overline{G}) = \overline{G}\gamma(\overline{P})$ and that the resulting representation $\text{rep}(\overline{P}, \overline{G})$ does not depend on the modification. The main result of this article is then the following.

Theorem A. — If $n \geq 1$, then $W_{k,a_p}(n)$ is nonempty and there exists $n(k, a_p) \geq 1$ with the property that if $n \geq n(k, a_p)$ and if $(\overline{P}, \overline{G})$ is the image of any $(P, G) \in W_{k,a_p}(n)$, then $\text{rep}(\overline{P}, \overline{G})^{\text{ss}} = \overline{V}_{k,a_p}^*$.

This theorem suggests the following algorithm. Choose some integer $n \geq 1$; since the set $M_2(\mathcal{O}_E[[X]]/(\pi_E^n, \varphi(X)^k))$ is finite, we can determine all the elements of $W_{k,a_p}(n)$ by checking for each pair of matrices (P, G) whether it satisfies conditions (1), (2), (3) and (4). For each pair $(P, G) \in W_{k,a_p}(n)$, we compute $\text{rep}(\overline{P}, \overline{G})^{\text{ss}}$. If we get two different k_E -linear representations from $W_{k,a_p}(n)$ in this way, then we replace n by $n + 1$; otherwise, $n = n(k, a_p)$ and $\overline{V}_{k,a_p}^* = \text{rep}(\overline{P}, \overline{G})^{\text{ss}}$. The theorem above ensures that the algorithm terminates and returns the correct answer. In order to implement the algorithm, we need to be able to identify $\text{rep}(\overline{P}, \overline{G})$ given P and G and one way of doing so is explained in §4.

The proof of theorem A is a simple application of the theory of Wach modules. Some background on (φ, Γ) -modules and Wach modules is given in §1. The main technical result showing that it is enough to work with truncated modules is proved in §2. Theorem A itself is proved in §3, and one way of determining $\text{rep}(P, G)$ from P and G is explained in §4. It is obvious that the algorithm sketched above is rather brutal, and that many improvements can be given; I have however chosen not to discuss the implementation of the algorithm. Note also that in order to have an effective algorithm, we would need to give a good estimate for $n(k, a_p)$. My guess is that $n(k, a_p) \approx e(E/\mathbf{Q}_p) \cdot k/(p - 2)$.

The algorithm can be modified in an easy way to work with $p = 2$. It can also be used to compute the reduction of all 2-dimensional crystalline irreducible representations of $\text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ since they are all twists of the V_{k,a_p} . It may be harder to generalize the

algorithm to higher dimensional cases or representations of $\text{Gal}(\overline{\mathbf{Q}_p}/F)$ with $F \neq \mathbf{Q}_p$ because one reason why the algorithm is so simple is that for 2-dimensional crystalline representations of $\text{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$, there is no parameter for the filtration.

1. (φ, Γ) -modules and Wach modules

Let $\Gamma \simeq \mathbf{Z}_p^\times$ be the group of the introduction and let \mathcal{A}_E be the π_E -adic completion of $\mathcal{O}_E[[X]][1/X]$, so that \mathcal{A}_E is the ring of power series $f(X) = \sum_{n \in \mathbf{Z}} a_n X^n$ with $a_n \in \mathcal{O}_E$ and $a_{-n} \rightarrow 0$ as $n \rightarrow +\infty$. The ring \mathcal{A}_E is endowed with an \mathcal{O}_E -linear frobenius φ given by $\varphi(f)(X) = f((1+X)^p - 1)$ and an action of Γ given by $\eta(f)(X) = f((1+X)^{\chi(\eta)} - 1)$ for $\eta \in \Gamma$. An étale (φ, Γ) -module (over \mathcal{O}_E) is a finite type \mathcal{A}_E -module D endowed with a semilinear frobenius such that $\varphi(D)$ generates D as an \mathcal{A}_E -module, and a commuting semilinear continuous action of Γ . By a theorem of Fontaine (see A.3.4 of [Fon90]), the category of étale (φ, Γ) -modules over \mathcal{O}_E is naturally isomorphic to the category of \mathcal{O}_E -linear representations of $\text{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$ and we denote the corresponding functor by $D \mapsto V(D)$, and the inverse functor by $V \mapsto D(V)$. If we restrict this equivalence of categories to objects killed by π_E , then we recover the equivalence described in the introduction.

An effective Wach module of height h is a free $\mathcal{O}_E[[X]]$ -module N of finite rank, endowed with a frobenius φ and an action of Γ such that :

1. $\mathcal{A}_E \otimes_{\mathcal{O}_E[[X]]} N$ is an étale (φ, Γ) -module;
2. Γ acts trivially on N/XN ;
3. $N/\varphi^*(N)$ is killed by Q^h .

If N is a Wach module, then we can associate to it the E -linear representation $V(N) = E \otimes_{\mathcal{O}_E} V(\mathcal{A}_E \otimes_{\mathcal{O}_E[[X]]} N)$. We can also define a filtration on N by $\text{Fil}^j N = \{y \in N \text{ such that } \varphi(y) \in Q^j \cdot N\}$ and the E -vector space $E \otimes_{\mathcal{O}_E} N/XN$ then has the structure of a filtered φ -module. By combining proposition III.4.2 and theorem III.4.4 of [Ber04], we get the following result.

Proposition 1.1. — *If N is an effective Wach module of height h , then $V(N)$ is a crystalline representation with Hodge-Tate weights in $[-h; 0]$, and $D_{\text{cris}}(V(N)) \simeq E \otimes_{\mathcal{O}_E} N/XN$. In addition, all crystalline representations with Hodge-Tate weights in $[-h; 0]$ arise in this way.*

Recall that $\mathcal{O}_E[[X]]/Q \simeq \mathbf{Z}_p[\zeta_p]$. The $\mathbf{Q}_p(\zeta_p)$ -vector space $E \otimes_{\mathcal{O}_E} N/QN$ is endowed with an action of Γ and by propositions III.2.1 and III.2.2 of [Ber04], we have the following result.

Proposition 1.2. — *If N is an effective Wach module, if $V(N)$ is the associated representation, viewed as a \mathbf{Q}_p -linear representation, and if $\eta \in \Gamma$ is such that $\chi(\eta) \in 1 + p\mathbf{Z}_p$, then there exists a basis of $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} N/QN$ over $\mathbf{Q}_p(\zeta_p)$ in which the matrix of η is diagonal and its coefficients on the diagonal are the $\chi(\eta)^{h_i}$ where h_1, \dots, h_d are the opposites of the Hodge-Tate weights of $V(N)$.*

If $V(N)$ is an E -linear representation with Hodge-Tate weights h_1, \dots, h_d then the Hodge-Tate weights of the underlying \mathbf{Q}_p -linear representations are the h_i 's each counted $[E : \mathbf{Q}_p]$ times; in particular, $\prod_{i=1}^d (\gamma_1 - \chi(\gamma_1)^{h_i}) = 0$ on $E \otimes_{\mathcal{O}_E} N/QN$ where $\gamma_1 = \gamma^{p-1}$.

2. Matrix lifting results

In this chapter, we give a proof of the main technical result which is used in order to justify that it is enough to work with truncations of (φ, Γ) -modules.

Proposition 2.1. — *If $1 \leq n \leq +\infty$ and P and G_k are two matrices in $M_d(\mathcal{O}_E/\pi_E^n[[X]])$ such that $\det(P) = Q^{k-1} \times \text{unit}$ and $G_k = \text{Id} \bmod X$ and $P\varphi(G_k) = G_k\gamma(P) \bmod \varphi(X)^k$, then :*

1. *there exists $G \in M_d(\mathcal{O}_E/\pi_E^n[[X]])$ such that $G = G_k \bmod X^k$ and $P\varphi(G) = G\gamma(P)$;*
2. *if P' and G' are two matrices equal to P and G modulo $\varphi(X)^k$ and X^k and satisfying the same conditions as P and G , then $\text{rep}(P', G') = \text{rep}(P, G)$.*

Proof. — We start by proving (1). Since $\det(P) = Q^{k-1} \times \text{unit}$, the same is true of $\det(\gamma(P))$ and hence we have $Q^{k-1}\gamma(P)^{-1} \in M_d(\mathcal{O}_E/\pi_E^n[[X]])$. We can therefore rewrite $P\varphi(G_k) = G_k\gamma(P) \bmod \varphi(X)^k$ as

$$G_k - P\varphi(G_k)\gamma(P)^{-1} \in X^k Q M_d(\mathcal{O}_E/\pi_E^n[[X]]),$$

since this is true after multiplying by Q^{k-1} and Q is not a zero divisor in $\mathcal{O}_E/\pi_E^n[[X]]$. Assume that $j \geq k$ and that we have a matrix G_j such that

$$G_j - P\varphi(G_j)\gamma(P)^{-1} = X^j R_j \in X^j M_d(\mathcal{O}_E/\pi_E^n[[X]]).$$

If $S_j \in M_d(\mathcal{O}_E/\pi_E^n)$ and if we set $G_{j+1} = G_j + X^j S_j$, then

$$\begin{aligned} G_{j+1} - P\varphi(G_{j+1})\gamma(P)^{-1} &= G_j - P\varphi(G_j)\gamma(P)^{-1} + X^j S_j - P X^j Q^j S_j \gamma(P)^{-1} \\ &= X^j (R_j + S_j - Q^{j-k+1} P S_j Q^{k-1} \gamma(P)^{-1}), \end{aligned}$$

and we can find S_j such that $R_j + S_j - Q^{j-k+1} P S_j Q^{k-1} \gamma(P)^{-1} \in X M_d(\mathcal{O}_E/\pi_E^n[[X]])$ since the map $S \mapsto S - p^{j-k+1} P(0) \cdot S \cdot (Q^{k-1} \gamma(P)^{-1})(0)$ is obviously a bijection from $M_d(\mathcal{O}_E/\pi_E^n)$ to itself. By induction on $j \geq k$, this allows us to find a sequence $(G_j)_{j \geq k}$ which converges for the X -adic topology to a matrix G satisfying (1).

In order to prove (2), we start by showing that there exists a matrix $M \in \mathrm{GL}_d(\mathcal{O}_E/\pi_E^n[[X]])$ such that $M^{-1}P'\varphi(M) = P$. We have by hypothesis $P' = P + \varphi(X)^k S$ and hence $P' = (1 + X^k R)P$ with $R = SQ^k P^{-1}$. By induction and successive approximations, we only need to show that if $P' = (1 + X^j R_j)P$ with $j \geq k$, then there exists $T_j \in \mathrm{M}_d(\mathcal{O}_E/\pi_E^n)$ such that $(1 + X^j T_j)^{-1} P' \varphi(1 + X^j T_j) = (1 + X^{j+1} R_{j+1})P$. We have

$$\begin{aligned} & (1 + X^j T_j)^{-1} \cdot (1 + X^j R_j) \cdot P \cdot \varphi(1 + X^j T_j) \\ &= (1 + X^j (R_j - T_j + Q^{j-k+1} P T_j Q^{k-1} P^{-1}) + O(X^{j+1})) \cdot P \end{aligned}$$

and the claim follows from the fact that $T \mapsto T - p^{j-k+1} P(0) \cdot T \cdot (Q^{k-1} P^{-1})(0)$ is obviously a bijection from $\mathrm{M}_d(\mathcal{O}_E/\pi_E^n)$ to itself. In order to prove (2), we are therefore reduced to the case $P = P'$. If we set $H = G'G^{-1}$, then the two equations $P\varphi(G) = G\gamma(P)$ and $P\varphi(G') = G'\gamma(P)$ give $P\varphi(H) = HP$, with $H = \mathrm{Id} \bmod X^k$. Let $H_0 = H$ and set $H_{m+1} = P\varphi(H_m)P^{-1}$. Since $H = \mathrm{Id} \bmod X^k$, we can write $H_0 = \mathrm{Id} + X^{k-1}\varphi^0(X)R_0$ and an easy induction shows that we can write $H_m = \mathrm{Id} + X^{k-1}\varphi^m(X)R_m$ with $R_m \in \mathrm{M}_d(\mathcal{O}_E/\pi_E^n[[X]])$ so that $H_m \rightarrow \mathrm{Id}$ as $m \rightarrow +\infty$. The equation $P\varphi(H) = HP$ implies that $H_m = H$ for all $m \geq 0$ and we are done. \square

3. Proof of the main theorem

In this chapter, we give a proof of theorem A, which we recall here.

Theorem 3.1. — *If $n \geq 1$, then $W_{k,a_p}(n)$ is nonempty and there exists $n(k, a_p) \geq 1$ with the property that if $n \geq n(k, a_p)$ and if $(\overline{P}, \overline{G})$ is the image of any $(P, G) \in W_{k,a_p}(n)$, then $\mathrm{rep}(\overline{P}, \overline{G})^{\mathrm{ss}} = \overline{V}_{k,a_p}^*$.*

Proof. — The representation V_{k,a_p}^* is a crystalline representation with Hodge-Tate weights $-(k-1)$ and 0 so that by proposition 1.1, there exists an effective Wach module N_{k,a_p} of height $k-1$ with the property that $V(N_{k,a_p}) \simeq V_{k,a_p}^*$. If P and G are the matrices of φ and γ in some basis of N_{k,a_p} then they obviously satisfy the equation $P\varphi(G) = G\gamma(P)$ and $G = \mathrm{Id} \bmod X$ by definition. The determinant of V_{k,a_p}^* is χ^{k-1} so that $\det(P) = Q^{k-1} \times u$ with $u \in 1 + X\mathcal{O}_E[[X]]$. The map $v \mapsto \varphi(v)/v$ from $1 + X\mathcal{O}_E[[X]]$ to itself is a bijection and since $p \neq 2$, every element of $1 + X\mathcal{O}_E[[X]]$ has a square root. We can therefore modify P and G accordingly so that $\det(P) = Q^{k-1}$. The fact that $D_{\mathrm{cris}}(V_{k,a_p}^*) = D_{k,a_p} = E \otimes_{\mathcal{O}_E} N_{k,a_p}/XN_{k,a_p}$ implies that $\mathrm{Tr}(P) = a_p \bmod X$. Finally by proposition 1.2, the operator $(\gamma_1 - 1)(\gamma_1 - \chi(\gamma_1)^{k-1})$ is zero on $E \otimes_{\mathcal{O}_E} N_{k,a_p}/QN_{k,a_p}$ so that if $G_1 = G\gamma(G) \cdots \gamma^{p-2}(G)$ and $\Pi(Y) = (Y-1)(Y-\chi(\gamma_1)^{(k-1)})$, then $\Pi(G_1) = 0 \bmod Q$. This shows that the images of P and G in $\mathrm{M}_2(\mathcal{O}_E[[X]]/(\pi_E^n, \varphi(X)^k))$ belong to $W_{k,a_p}(n)$ for all $n \geq 1$ so that $W_{k,a_p}(n)$ is nonempty.

We now prove the existence of $n(k, a_p)$. There are only finitely many semisimple k_E -linear 2-dimensional representations of $\text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ so that if for infinitely many n there exists $(P, G) \in W_{k, a_p}(n)$ whose image $(\overline{P}, \overline{G})$ satisfies $\text{rep}(\overline{P}, \overline{G})^{\text{ss}} \neq \overline{V}_{k, a_p}^*$ then there exists some semisimple k_E -linear 2-dimensional representation U of $\text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ which arises from $(P, G) \in W_{k, a_p}(n)$ for infinitely many n 's. By a standard compactness argument (recall that the $W_{k, a_p}(n)$ are finite sets), this implies that we can find a compatible sequence $(P_n, G_n)_{n \geq 1}$ with each term “reducing mod π_E ” to U . The P_n and the G_n converge to P and G in $M_2(\mathcal{O}_E[[X]])$ and P and G still satisfy conditions (1), (2), (3) and (4) of the definition of $W_{k, a_p}(n)$ since these conditions are continuous. In particular, conditions (1), (2) and the first part of (3) imply that P and G define a Wach module, which then comes from a crystalline representation V . Condition (3) then implies that $D_{\text{cris}}(V) \simeq D_{k, a_p}$ as φ -modules while condition (4) along with proposition 1.2 implies that the Hodge-Tate weights of V belong to $\{0; -(k-1)\}$. The fact that $D_{\text{cris}}(V) \simeq D_{k, a_p}$ implies that the sum of the weights is $-(k-1)$ so that $D_{\text{cris}}(V) \simeq D_{k, a_p}$ as filtered φ -modules and hence $V \simeq V_{k, a_p}^*$. But then $U = \overline{V}^{\text{ss}} = \overline{V}_{k, a_p}^*$ which is a contradiction. This shows the existence of $n(k, a_p)$ and finishes the proof of the theorem. \square

4. Identifying mod p representations

If P and G are two matrices in $M_2(k_E[[X]])$ such that $\det(P) = Q^{k-1} \times \text{unit}$ and $G = \text{Id} \bmod X$ and $P\varphi(G) = G\gamma(P) \bmod \varphi(X)^k$, then by proposition 2.1 there is a well-defined k_E -linear representation $\text{rep}(P, G)$ associated to P and G . In this chapter, we give a crude method for determining which one it is. Recall that if V is a k_E -linear representation of $\text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, then by B.2.1 of [Fon90] there is a $k_E[[X]]$ -lattice $D^+(V)$ inside $D(V)$ which is stable under φ and the action of Γ and such that any other such lattice N satisfies $N \subset D^+(V)$. If M is the matrix of a basis of N in a basis of $D^+(V)$ then $\det(\varphi|N) = \det(\varphi|D^+(V)) \cdot \varphi(\det(M))/\det(M)$. In particular, if $\det(\varphi|N)$ is $Q^{k-1} \times \text{unit}$ then $\det(M)$ divides X^{k-1} . The algorithm for determining $\text{rep}(P, G)$ is then the following :

1. make a list of all the finitely many k_E -linear 2-dimensional representations of $\text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$;
2. for each of them, compute P and G , the matrices of φ and γ on $D^+(V)$ to precision $X^{(p+1)k+k-1}$;
3. make a list of all the $M^{-1}P\varphi(M)$ and $M^{-1}G\gamma(M)$ for the finitely many $M \in M_2(k_E[[X]]/X^{(p+1)k+k-1})$ such that $\det(M)$ divides X^{k-1}

Step (2) is an interesting exercise in (φ, Γ) -modules. Note also that in step (3) we need to multiply by M^{-1} so that the precision drops from $X^{(p+1)k+k-1}$ to $X^{(p+1)k} = \varphi(X)^k$.

This procedure gives a complete list of all possible (P, G) with the corresponding representation and given a pair (P, G) , the representation $\text{rep}(P, G)$ can then be determined by a simple table lookup.

References

- [Ber04] L. BERGER – “Limites de représentations cristallines”, *Compos. Math.* **140** (2004), no. 6, p. 1473–1498.
- [Ber05] ———, “Représentations modulaires de $\text{GL}_2(\mathbf{Q}_p)$ et représentations galoisiennes de dimension 2”, *Astérisque*, to appear, 2005.
- [BG09] K. BUZZARD & T. GEE – “Explicit reduction modulo p of certain crystalline representations”, *IMRN*, to appear, 2009.
- [BLZ04] L. BERGER, H. LI & H. J. ZHU – “Construction of some families of 2-dimensional crystalline representations”, *Math. Ann.* **329** (2004), no. 2, p. 365–377.
- [Bre03] C. BREUIL – “Sur quelques représentations modulaires et p -adiques de $\text{GL}_2(\mathbf{Q}_p)$. II”, *J. Inst. Math. Jussieu* **2** (2003), no. 1, p. 23–58.
- [CF00] P. COLMEZ & J.-M. FONTAINE – “Construction des représentations p -adiques semistables”, *Invent. Math.* **140** (2000), p. 1–43.
- [Fon90] J.-M. FONTAINE – “Représentations p -adiques des corps locaux. I”, *The Grothendieck Festschrift, Vol. II*, *Progr. Math.*, vol. 87, Birkhäuser Boston, Boston, MA, 1990, p. 249–309.

July 2009

LAURENT BERGER, Université de Lyon, UMPA ENS Lyon, 46 allée d'Italie, 69007 Lyon, France
E-mail : laurent.berger@ens-lyon.fr • *Url* : www.umpa.ens-lyon.fr/~lberger/